Federal PKI
Management Authority
Enabling Trust

Path Discovery and Validation (PD-VAL) Product Conformance

TECHNICAL TEST REPORT

[Mount Airey Ozone Server]

VERSION 1.0

June 12, 2014

FINAL

PREPARED BY PROTIVITI GOVERNMENT SERVICES
FOR GENERAL SERVICES ADMINISTRATION

TABLE OF CONTENTS

TABLES

1 Scope and Specifications

The Federal Public Key Infrastructure Management Authority (FPKIMA) tested Mount Airey's Ozone Server against the National Institute of Standards and Technology (NIST) Public Key Infrastructure (PKI) test suite Public Key Interoperability Test Suite (PKITS) for Certification Path Validation; Version 1.0.1; April 14, 2011 and NIST Recommendation for X.509 Path Validation

1.1 Product Description

The Mount Airey Ozone Server is an Authorization Service within the Ozone Application Suite that acts as a XACML-based Policy Decision Point (PDP). It uses a standards-based web service interface (SOAP 1.1) run on Java to perform verification requests from an application. To make an access control decision, the Ozone server uses an Action ID to send a request to the Authorization Service containing a Resource ID indicating the requested proof, and a Subject Certificate to be authorized. The Ozone Server works with the Ozone Authority which contains a set of periodically updated proofs based on a specified trust anchor and a pre-configured set of CRLs and CA certificates built using the internal RSA jSafe library. The Server returns a "Permit" or "Deny" authorization response to the application based on the proof verified. The Ozone Server is also hard-coded with a default deny-all policy fail safe for any situation where there is a server-side error in resolving a Resource ID (i.e. a proof).

1.2 Technical Specifications

Specifications of the Ozone Server used to execute the tests are as follows:

a) Relevant software version: Ozone Server 2013 Version 2.1.301, build 221
   (1) Ozone Server 2.1.301 with RSA BSafe Crypto-J library v6.0.0.1 was provided by Ozone on 12/04/2013
b) Ozone Server was implemented on an FPKIMA Test Server:
   (1) CPU: Dual Intel(R) Xeon(R) @ 3.00 GHz
   (2) RAM: 2.00 GB
   (3) Operating System: CentOS Linux 6.4

Specifications of client used to execute the tests:

a) Ozone Validation Tester 1.0.51.21, provided by Ozone on 12/4/2013
b) Ozone Validation Tool was implemented and run from a computer with the following specs:
   (1) CPU: Intel(R) Core(TM) 2 i5 @ 2.40GHz
   (2) RAM: 4.00 GB
   (3) Operating System: 64 Bit Windows 7 Enterprise

2 Path Validation Testing Program Report

In NIST Recommendation for X.509 Path Validation, some tests are identified as applicable to all applications, some are identified as applicable to applications that support particular services, and some are identified as not necessary to run. The tests that are not necessary to run are intended to be useful in evaluating particular application features that may or may not be supported. Competent applications that are compliant with all relevant standards may not necessarily pass these tests. These tests were included in this testing process, and are referred to as the "non-required" tests.

The following subsections summarize the tests that were executed:

a) Section 2.1 describes testing with all of the CA certificates and CRLs imported into the Ozone Server Trust Manager.

2.1 Testing with all CA Certificates and CRLs Stored in Ozone Server

a) All CA certificates and CRLs were installed (or attempted to be installed) in the Ozone Server, so certificate path building and validation could be performed at the Ozone Server with no need to follow the certificate references to external locations.

b) Some tests did not allow the import of the associated CRLs, for the same reasons that the test is expected to produce an invalid response. These tests then produce an invalid response because there is no CRL available for validation. This is considered an acceptable response.

c) Results using this configuration:
   - Total number of tests = 247
     (i) Number of baseline tests = 129
     (ii) Number of optional tests = 118
   - Number of tests that return the appropriate expected validation response ("Success" or "Failed"), as indicated in the Test Suite document = 247
   - Total number of applicable issues = 0
   - Table 1 details the PKITS Path Validation Test Issues

TABLE 1 PKITS PATH VALIDATION TEST ISSUES – STATIC DATA

PKITS PATH VALIDATION TEST ISSUES – STATIC DATA	
4.1 Signature Verification	All tests passed delivering expected result.
4.2 Validity Periods	All tests passed delivering expected result.
4.3 Verifying Name Chaining	All tests passed delivering expected result.
4.4 Basic Certificate Revocation Tests	All tests passed delivering expected result.
4.5 Verifying Paths with Self-Issued Certificates	All tests passed delivering expected result.
4.6 Verifying Basic Constraints	All tests passed delivering expected result.
4.7 Key Usage	All tests passed delivering expected result.
4.8 Certificate Policies	All tests passed delivering expected result. See miscellaneous comments for additional information.
4.9 Require Explicit Policy	All tests passed delivering expected result.
4.10 Policy Mappings	All tests passed delivering expected result. See miscellaneous comments for additional information.
4.11 Inhibit Policy Mapping	All tests passed delivering expected result.
4.12 Inhibit Any Policy	All tests passed delivering expected result.
4.13 Name Constraints	All tests passed delivering expected result. See miscellaneous comments for testing anomalies.
4.14 Distribution Points	All tests passed delivering expected result.
4.15 Delta-CRLs	All tests passed delivering expected result.
4.16 Private Certificate Extensions	All tests passed delivering expected result.

2.2 Miscellaneous Comments

Eight tests (4.8.15, 4.8.16, 4.8.17, 4.8.18-1, 4.8.18-2, 4.8.19, 4.10.13, and 4.10.14) involve User Notice Qualifiers in the Certificate Policies extension of certificates, with specific user notices expected to be displayed depending on the certificate policy processing if the product supports it. Each of these tests is identified in NIST Recommendation for X.509 Path Validation as a non-required test (or the test is required, while the user notice portion of the test is identified as "irrelevant"). Although Ozone Server does not display the user notices and does not appear to support this feature, all eight of these tests returned the appropriate expected validation response ("Success").

In the invalid name constraints tests, Ozone Server successfully marked the certificate as invalid, but the error message generated always stated a Subject Alternative Name (SAN) even when the SAN was not the attribute tested. Conclusive testing of the twelve optional name constraint tests (4.13.2, 4.13.7 – 4.13.10, 4.13.12, 4.13.13, 4.13.15 – 4.13.17, 4.13.20, 4.13.29), showed it is a problem with the error message and not the validation testing. All twelve tests returned the appropriate response of "invalid", however the error message may be misleading when the name constraints error is a result of either the Subject DN or a CA certificate in the chain. The vendor has responded revealing this is an issue with the underlying library from RSA and is expected to be corrected in a future version of RSA.

The User Notice Qualifiers and Invalid Name Constraint tests mentioned above are optional test cases and are not required to achieve product approval. The optional test cases are designed to test how a product responds to requests for non-supported services. The product is required to output an appropriate response and an appropriate response for the wrong reason is considered passing.

3 PRODUCT DECISION

The FPKIMA considers these test results to be sufficient and appropriate and recommend the Mount Airey Ozone Server to be added to the FPKI PDVAL Product List (PPL).